H 35. Transpositionen tun sich zusammen: Gemeinsam sind wir stark.
Gegeben sei die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 8 & 1 & 9 & 2 & 10 & 3 & 11 & 4 & 12 & 5 & 13 & 6 & 14 & 7 \end{pmatrix} \in S_{14}.$$

1.) Schreiben Sie π als Produkt von paarweise elementfremden Zyklen.

2.) Stellen Sie π als Produkt von Transpositionen dar.

3.) Welches Signum besitzt π?

4.) Es sei $n \in \mathbb{N}$. Stellen Sie den Zykel $(1\ 2\ 3 \dots n) \in S_n$ als Produkt von Transpositionen dar. Welches Signum hat $(1\ 2\ 3 \dots n)$?

1) $\pi = (1\ 8\ 4\ 2) \circ (3\ 9\ 12\ 6) \circ (5\ 10) \circ (7\ 11\ 13\ 14)$

$\pi(1) = 8,\ \pi(8) = 4,\ \pi(4) = 2,\ \pi(2) = 1$ usw.

2) k-Zykel $(x_1\ x_2\ x_3 \dots x_k) = \underbrace{(x_1 x_2) \circ (x_2 x_3) \circ (x_3 x_4) \circ \dots \circ (x_{k-1} x_k)}_{k-1 \text{ Transpositionen (2-Zykel)}}$

$\pi = (1\,8) \circ (8\,4) \circ (4\,2) \circ (3\,9) \circ (9\,12) \circ (12\,6) \circ (5\,10) \circ (7\,11) \circ (11\,13) \circ (13\,14)$

3) $\operatorname{Sign} \pi = (-1)^{\text{Anzahl der Transpositionen}} = (-1)^{10} = 1$

oder mit Hilfe von Fehlständen, d.h. der Anzahl der Paare (i,j), $i,j \in E_n$ mit $i<j$ und $f(i) > f(j)$: $\operatorname{Sign} \pi = (-1)^{|F(f)|} = (-1)^{28} = 1$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 8 & 1 & 9 & 2 & 10 & 3 & 11 & 4 & 12 & 5 & 13 & 6 & 14 & 7 \end{pmatrix}$$

$F(f) = \{(1,2), (1,4), (1,6), (1,8), (1,10), (1,12), (1,14), (3,4), (3,6), (3,8), (3,10), (3,12), (3,14), (5,6), (5,8), (5,10), (5,12), (5,14), (7,8), (7,10), (7,12), (7,14), (9,10), (9,12), (9,14), (11,12), (11,14), (13,7)\} \Rightarrow |F(f)| = 28.$

Frage: Warum gilt für alle Permutationen f: $\operatorname{Sign}(f^2) = 1$?

4) Es gilt: $(1\ 2\ 3\ 4\ 5 \dots n) = \underbrace{(12)(23)(34) \dots (n-1, n)}_{n-1 \text{ Transpositionen}}$

$\Rightarrow \operatorname{Sign}(123 \dots n) = (-1)^{n-1}$

H 36. Klein ist fein.

Gegeben sei die Teilmenge

$$V_4 := \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \right\} \subseteq S_4.$$

Zeigen Sie:

- V_4 ist eine Untergruppe von S_4.
- V_4 ist isomorph zur Gruppe derjenigen Drehbewegungen, die einen Ziegelstein mit unterschiedlicher Länge, Breite und Höhe deckungsgleich auf sich selbst abbilden.

V_4 heißt KLEINsche Vierergruppe und ist bis auf Isomorphie die einzige nichtzyklische Gruppe mit vier Elementen.

Wir benennen die 4 Elemente von V_4 mit $id = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ und

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)\circ(34)$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)\circ(24)$, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)\circ(23)$,

wobei wir statt der angegebenen Wertschreibweise auch die Zyklenschreibweise verwenden können.

1) Wir zeigen: V_4 ist Untergruppe der S_4 mit Hilfe des Untergruppenkriteriums

- V_4 ist offensichtlich nicht die leere Menge
- Inversenbildung: Wegen $\sigma^2 = \tau^2 = \pi^2 = id$ (Produkte elementfremder 2-Zykel) gilt: $\sigma^{-1} = \sigma$, $\tau^{-1} = \tau$, $\pi^{-1} = \pi$ liegen jeweils in V_4.
- Abgeschlossenheit: Durch Nachrechnen findet man: $\sigma \circ \tau = \pi$ (1)

  Multiplikation von (1) mit σ von links liefert: $\sigma\circ\sigma\circ\tau = \sigma\circ\pi \overset{\sigma^2=id}{\Rightarrow} \tau\circ\pi = \tau$ (2)

  Multiplikation von (2) mit π von rechts liefert: $\sigma\circ\pi\circ\pi = \tau\circ\pi \overset{\pi^2=id}{\Rightarrow} \tau\circ\pi = \sigma$ (3)

$\circ$	id	σ	τ	π
id	id	σ	τ	π
σ	σ	id	π	τ
τ	τ	π	id	σ
π	π	τ	σ	id

  u.s.w liefert die angegebene Gruppentafel, woraus die Abgeschlossenheit ersichtlich ist.

Bemerkung: V_4 ist kommutative Untergruppe der nicht kommutativen Gruppe S_4 und isomorph zur Kleinschen Vierergruppe (P10).

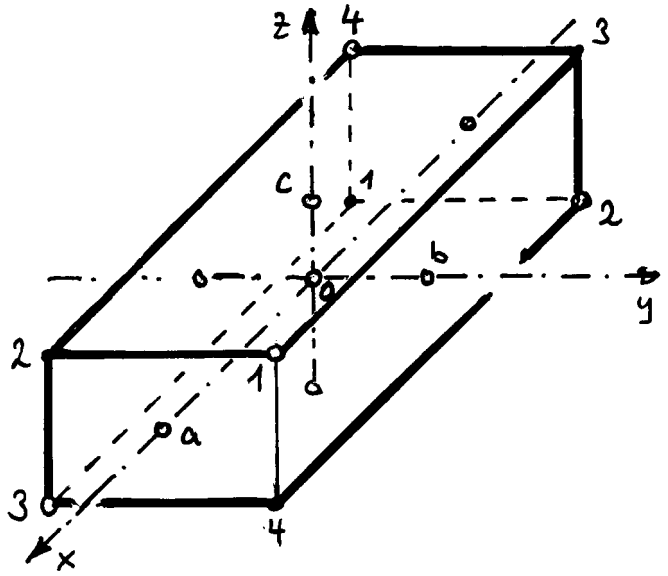
2) In einem rechtwinkligen xyz-Koordinatensystem bilden die Punkte $(\pm a, \pm b, \pm c)$ die 8 Ecken eines Quaders (Ziegelstein) o.E. mit $a > b > c > 0$, der nur durch Rotation um eine der 3 Koordinatenachsen mit 180° oder die Identität deckungsgleich auf sich abgebildet wird.

Da die zweifache 180°-Drehung um eine der 3 Achsen gleich der Identität ist (*) und die Komposition (Hintereinanderausführung) der 180°-Drehungen um zweier drei Achsen die 180°-Drehung um die dritte Achse liefert, bilden die 4 Abbildungen (!) eine Gruppe mit 4 Elementen, die wegen (*) isomorph zur Kleinschen Vierergruppe und damit zu V_4 ist.

Beachte: Nach P10 gibt es bis auf Isomorphie genau eine Gruppe G mit $|G|=4$ Elementen und $x^2 = e \ \forall x \in G$!

Zusatz: Direkte Angabe der Isomorphie:

Aufgrund der Punktsymmetrie des Quaders zum Ursprung $O=(0,0,0)$ liegen nach jeder dieser Rotationen die Bilder der beiden Punkte $\pm(a,b,c)$ wieder einander gegenüber. Daher identifizieren wir gegenüberliegende Ecken des Quaders und bezeichnen die beiden Ecken $\pm(a,b,c)$ mit 1
die beiden Ecken $\pm(-a,b,-c)$ mit 2
die beiden Ecken $\pm(a,-b,-c)$ mit 3
die beiden Ecken $\pm(-a,-b,c)$ mit 4.



Der 180°-Drehung:
um die x-Achse entspricht dann die Permutation $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$
um die y-Achse entspricht dann die Permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$
um die z-Achse entspricht dann die Permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

Dass die Zuordnung (Abbildung) strukturerhaltend (d.h. homomorph) ist, kann man direkt nachrechnen.

H 37. Andere Ringe als $\mathbb{Z}$

1. Geben Sie einen Ring ohne Eins an.
2. Geben Sie einen Ring mit Nullteilern an.

Begründen Sie kurz, warum Ihr Beispiel ein Ring ist.

1. Behauptung $\{n\cdot\mathbb{Z}, +, \cdot\}$ mit $1<n\in\mathbb{N}$ ist ein Ring ohne Eins!

Begründung: $n\cdot\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\} \subset \mathbb{Z}$ (klar) und es gilt:

(i) $(n\cdot\mathbb{Z}, +)$ ist kommutative Gruppe, da Untergruppe von $(\mathbb{Z}, +)$

(a) $a,b \in n\mathbb{Z} \Leftrightarrow \exists p,q\in\mathbb{Z}: a=p\cdot n, b=q\cdot n \Rightarrow a+b=(p+q)\cdot n \Rightarrow a+b\in n\cdot\mathbb{Z}$

(b) zu $a=p\cdot n\in n\mathbb{Z}$ ist $a^{-1}=(-p)\cdot n\in n\cdot\mathbb{Z}$ das Inverse

(ii) Multiplikation $\cdot$ ist abgeschlossen, assoziativ und distributiv

(a) $a,b\in n\mathbb{Z} \Leftrightarrow \exists p,q\in\mathbb{Z}: a=p\cdot n, b=q\cdot n \Rightarrow a\cdot b=(p\cdot q\cdot n)\cdot n \Rightarrow a\cdot b\in n\mathbb{Z}$

Für alle $a,b,c\in n\mathbb{Z}$ gilt: $a=p\cdot n$, $b=q\cdot n$, $c=r\cdot n$ mit $p,q,r\in\mathbb{Z}$ und:

(b) $[a\cdot b]\cdot c = (p\cdot n\cdot q\cdot n)\cdot r\cdot n = p\cdot n\cdot(q\cdot n\cdot r\cdot n) = a\cdot(b\cdot c)$

Assoziativität in $(\mathbb{Z}, +, \cdot)$!

(c_1) $(a+b)\cdot c = (p\cdot n+q\cdot n)\cdot r\cdot n = p\cdot n\cdot r\cdot n + q\cdot n\cdot r\cdot n = a\cdot c + b\cdot c$

(c_2) $a\cdot(b+c) = p\cdot n\cdot(q\cdot n+r\cdot n) = p\cdot n\cdot q\cdot n + p\cdot n\cdot r\cdot n = a\cdot b + a\cdot c$

Distributivität in $(\mathbb{Z}, +, \cdot)$!

Man sagt: Die Assoziativität und Distributivität von $(n\cdot\mathbb{Z}, +, \cdot)$ wird aus $(\mathbb{Z}, +, \cdot)$ geerbt.

Annahme $\exists e\in n\cdot\mathbb{Z}$ mit $e\cdot a = a$ für ein $a\in n\mathbb{Z}\setminus\{0\}$

$\Leftrightarrow \exists p,q\in\mathbb{Z}: e=p\cdot n, a=q\cdot n$ mit $p\cdot q\cdot n^2 = q\cdot n$ $(n>1, q\neq 0)$

$\Leftrightarrow n\cdot p = 1$ ↯ $\Rightarrow$ Es gibt kein Einselement im Ring $\{n\cdot\mathbb{Z}, +, \cdot\}$

2. Behauptung $\{\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}, \oplus_n, \odot_n\}$ ist für $n=p\cdot q$ mit $1<p,q\in\mathbb{N}$ ein Ring mit Nullteilern ($\mathbb{Z}_n = \{0,1,2,\ldots,(n-1)\}$ & Rechnen modulo n)

Begründung:

(i) $(\mathbb{Z}_n, \oplus_n)$ ist kommutative Gruppe nach Vorlesung bzw. Modulorechnen.

(ii) Multiplikation $\odot_n$ ist abgeschlossen, assoziativ und distributiv

vgl. Modulo rechnen

Wegen $n=p\cdot q$ mit $1<p,q\in\mathbb{N}$ gilt:

$p\odot_n q = p\cdot q \bmod n = n \bmod n = 0 \Rightarrow$ p und q sind Nullteiler in $\mathbb{Z}_n$!

H 38. Bestimmen Sie bis auf Isomorphie alle Körper mit 3 bzw. 4 Elementen.

K ist ein Körper $\Leftrightarrow$ $\cdot$ $(K,+)$ und $(K\setminus\{0\},\cdot)$ sind abelsche Gruppen
$\cdot$ $(K,+,\cdot)$ ist distributiv

K muss ein neutrales Element der Addition, die Null 0, und ein neutrales Element der Multiplikation, die Eins $1\neq 0$, enthalten $\Rightarrow$

1.) 3 elementiger Körper $K_3=\{0,1,a\}$

hat nach P10 folgende Gruppentafeln (bis auf Isomorphie eindeutig)

+	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

·	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

beide abelsch ✓ ·

Wegen Kommutativität genügt es, ein Distributivgesetz zu zeigen

$x\cdot(y+z) = x\cdot y + x\cdot z$

$1 = a\cdot(1+1) = a\cdot 1 + a\cdot 1 = 1$

$0 = a\cdot(1+a) = a\cdot 1 + a\cdot a = 0$

$a = a\cdot(a+a) = a\cdot a + a\cdot a = a$

Für $x=0$ und $x=1$ gilt Gleichheit

Für $x=a$ und $y=0 \vee z=0$ gilt die Gleichheit, daher verbleiben wegen der Kommutativität 3 Fälle zu prüfen

Beispiel: $K_3 = \mathbb{Z}_3 = \{0,1,2\}$ mit $\oplus_3$, $\odot_3$ bis auf Isom. eindeutig

2.) 4 elementiger Körper $K_4=\{0,1,a,b\}$

Nach P10 hat $(K_4\setminus\{0\},\cdot)$ bis auf Isomorphie nebenstehende Gruppentafel. Für $(K_4,+)$ stehen zwei Tafeln zur Wahl!

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

abelsch!

Wie muss unter Berücksichtigung der Distributivität die Gruppentafel für $(K,+)$ aussehen? Insbesondere die Einträge x,y,z?

+	0	1	a	b
0	0	1	a	b
1	1	x		
a	a		y	
b	b			z

$\Rightarrow x = 1+1 = 0 \wedge$

$a+1 = 1+a = b \wedge$

$b+1 = 1+b = a$

Annahme: $x = 1+1 = a \Rightarrow y = a+a = a(1+1) = a\cdot a = b$

$\Rightarrow$ y in Gruppentafel beim Eintrag von b in 2. Zeile!

Annahme: $x = 1+1 = b \Rightarrow z = b+b = b(1+1) = b\cdot b = a$

$\Rightarrow$ y in Gruppentafel beim Eintrag von a in 2. Zeile!

Annahme: $y = a+a = 1 \Rightarrow a = a(a+a) = aa+a\cdot a = b+b$ (11 = z)

$\Rightarrow$ y in Gruppentafel 3. Zeile oder 3 Spalte!

$\Rightarrow y = a+a = 0 \wedge z = b+b = 0 \wedge a+b = b+a = 1$

$\Rightarrow (K_4,+)$ ist isomorph zur Kleinschen Vierergruppe ✓

Wegen Kommutativität genügt es, ein Distributivgesetz zu zeigen:

$x\cdot(y+z) = x\cdot y + x\cdot z$

$1 = a\cdot(1+a) = a\cdot 1 + a\cdot a = 1$

$b = a\cdot(1+b) = a\cdot 1 + a\cdot b = b$

$a = a\cdot(a+b) = a\cdot a + a\cdot b = a$

$a = b\cdot(1+a) = b\cdot 1 + b\cdot a = a$

$1 = b\cdot(1+b) = b\cdot 1 + b\cdot b = 1$

$b = b\cdot(a+b) = b\cdot a + b\cdot b = b$

Für $x=0$ und $x=1$ gilt Gleichheit

Für $y=0 \vee z=0$ gilt die Gleichheit

Für $y=z$ gilt wegen $y+y=0$ die Gleichheit, daher verbleiben wegen der Kommutativität 6 Fälle zu prüfen.

Beispiel: $K_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$ bis auf Isomorphie eindeutig.

$K_4 = \{(0,0), (0,1), (1,0), (1,1)\}$ mit

(0,0): Null, (0,1): Eins, (1,0): a, (1,1): b

Addition: $(a,b) \oplus (c,d) = (a \oplus_2 b, c \oplus_2 d)$ und

Multiplikation $(a,b) \odot (c,d) = (a\cdot d \oplus_2 b\cdot c \oplus_2 ac, ac \oplus_2 bd)$

Zur Übung nachrechnen !

Beachte: • $K_4 \neq \mathbb{Z}/4\mathbb{Z}$ Restklassenring, der kein Körper ist, da $2 \odot_4 2 = 0$ und insbesonder $1 \oplus_4 1 = 2 \neq 0$!

• In K_4 gilt: $x + x = 0 \quad \forall x \in K_4$!

Zusatz: • K_4 ist auch isomorph zum Körper der Polynome $\mathbb{Z}_2(t)$ modulo $f = t^2+t+1$ (f in $\mathbb{Z}_2$ irreduzibel) mit den Elementen $\{0, 1, t, t+1\}$ und den Gruppentafeln

+	0	1	t	t+1
0	0	1	t	t+1
1	1	0	t+1	t
t	t	t+1	0	1
t+1	t+1	t	1	0

da in $\mathbb{Z}_2(t)$ gilt:

$1+1=0$ und

$t+t = t\cdot(1+1) = 0$

·	0	1	t	t+1
0	0	0	0	0
1	0	1	t	t+1
t	0	t	t+1	1
t+1	0	t+1	1	t

da in $\mathbb{Z}_2(t)$ modulo f gilt:

$t^2 =_f \underbrace{(t^2+t+1)}_{=0} + t + 1 =_f t+1 \Rightarrow$

$t\cdot(t+1) =_f t^2 + t =_f t+1+t =_f 1$

und $(t+1)(t+1) =_f t^2 + \underbrace{t+t}_{=0} + 1 =_f t+1+1 =_f t$